The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method of processing a Session Initiation Protocol (SIP) message, the method comprising:

(a) receiving a SIP request at a SIP node, the SIP request including a message header;

(b) generating a signature based upon at least a portion of the message header;

(c) generating a SIP node header entry; and

(d) inserting the signature into the SIP node header entry.

2. The method of claim 1, wherein the SIP node header entry is an echoed header.

3. The method of claim 2, wherein the portion of the message header includes data indicative of network routing locations.

4. The method of claim 1, wherein the SIP node header entry is a VIA header.

5. The method of claim 4, further comprising:

(e) receiving a SIP response at the SIP node in reply to the SIP request, the SIP response comprising the VIA header for the SIP node, the VIA header including a first received signature; and

(f) verifying the first received signature.

6. The method of claim 5, wherein verifying includes generating a verification signature based upon at least one VIA header of the SIP response and comparing the verification signature with the first received signature.

7. The method of claim 5, further comprising:

(g) determining a next link to a next SIP node to receive the SIP request; and

(h) determining if the next link to the next SIP node is an untrusted link, wherein generating the first signature includes only generating the first signature if the next link is an untrusted link.

8. The method of claim 1, wherein generating the signature includes generating a first signature based upon at least one VIA header of the message header.

9. The method of claim 8, wherein generating the first signature is based upon at least one VIA header of the message header and at least one of a peer FQDN, a connection identifier of the connection over which the message will be sent on a next hop, at least a portion of a FROM header of the message header, at least a portion of a TO header of the message header, at least a portion of a CALL-ID header of the message header, and at least a portion of a CSeq header of the message header.

10. The method of claim 8, wherein the message header includes a plurality of VIA headers and generating the first signature includes generating the first signature based upon the plurality of VIA headers except the VIA header of the SIP node.

11. The method of claim 1, wherein generating the signature includes generating a second signature based upon at least a portion of a RECORD-ROUTE header and at least a portion of a CONTACT header of the message header.

12. The method of claim 11, wherein inserting the signature includes inserting the second signature as a URI parameter into a RECORD-ROUTE header of the SIP node.

13. The method of claim 11, wherein generating the second signature includes generating a second signature based on a URI portion of each RECORD-ROUTE header in the message header except for a RECORD-ROUTE header of the SIP node, and a URI portion of the CONTACT header in the message header.

14. The method of claim 1, further comprising:

(j) receiving a SIP response in reply to the SIP request, the SIP response including a response header;

(k) generating a fourth signature based upon a RECORD-ROUTE header and a CONTACT header of the response header; and

(l) inserting the fourth signature into a RECORD-ROUTE header of the SIP node of the response.

15. The method of claim 14, further comprising before generating the fourth signature, removing an existing signature from the SIP node header entry.

16. The method of claim 14, wherein inserting the fourth signature includes inserting the fourth signature as a URI parameter into the RECORD-ROUTE header of the SIP node.

17. The method of claim 14, wherein generating the fourth signature includes generating the fourth signature based upon the URI portions of each RECORD-ROUTE header of the response except for the RECORD-ROUTE header of the SIP node, and a URI portion of the CONTACT header.

18. The method of claim 14, further comprising:

(n) determining a next link to a next SIP node to receive the SIP request; and

(o) determining if the next link to the next SIP node is an untrusted link, wherein generating the second signature includes only generating the second signature if the next link is an untrusted link.

19. The method of claim 18, wherein the SIP node is within a pool of servers and the method further comprises inserting an encrypted session key into the RECORD-ROUTE header of the SIP node.

20. The method of claim 1, further comprising:

(p) determining a RECORD-ROUTE header of the SIP request; and wherein generating the signature includes generating a third signature based upon at least a portion of the RECORD-ROUTE header of the SIP request.

21. The method of claim 20, wherein inserting the third signature includes inserting the third signature into a RECORD-ROUTE header of the SIP node.

22. The method of claim 21, wherein inserting the third signature includes inserting the third signature as a header parameter of the RECORD-ROUTE header of the SIP node.

23. The method of claim 21, further comprising:

(s) receiving a SIP response at the SIP node in reply to the SIP request, the SIP response comprising the RECORD-ROUTE header for the SIP node which includes a third received signature; and

(t) verifying the third received signature.

24. The method of claim 20, further comprising:

(q) determining a next link to a next SIP node to receive the SIP request; and

(r) determining if the next link to the next SIP node is an untrusted link, wherein generating the third signature includes only generating the third signature if the next link is an untrusted link.

25. A computer readable medium having computer executable steps for performing the steps in claim 1.

26. A computer readable medium having computer executable instructions for performing steps for processing messages in a pool of servers having a first server and a second server which are constructed and arranged to be interchangeably used to process messages in the same dialog, the steps comprising:

(a) identifying, at the first server, a public key and a private key;

(b) receiving, at the first server, a first message including a first header;

(c) generating a session key;

(d) encrypting the session key with the private key;

(e) generating, with the public key, a key signature based on the encrypted session key;

(f) inserting the key signature into the first header.

27. The computer readable medium of claim 26, further comprising:

(g) identifying, at the second server, the public key and the private key;

(h) receiving, at the second server, a second message including a second header, the second header comprising the key signature;

(i) decrypting the key signature to determine the session key.

28. The computer readable medium of claim 27, further comprising:

(j) verifying at least a portion of the second message with the session key.

29. The computer readable medium of claim 26, wherein the first message is a Session Initiation Protocol (SIP) message.

30. The computer readable medium of claim 26, wherein the first server is a proxy server.

31. The computer readable medium of claim 26, further comprising identifying a time stamp containing data representing a date and time of creation for the session key and

appending the time stamp to the session key, wherein encrypting the session key includes encrypting the session key and the time stamp.

32. A computer readable medium having stored thereon a data structure representing a Session Initiation Protocol (SIP) request, the data structure comprising:

(a) a plurality of SIP headers comprising an echoed header including an address of a SIP node in a route for the SIP request and data representing a digital signature generated by signing a portion of the SIP headers with a session key, wherein the echoed header is selected from the group consisting of a VIA header, a FROM header, a TO header, a RECORD-ROUTE header, a CALL-ID header, and a CSeq header.

33. The computer readable medium of claim 32, wherein the plurality of SIP headers comprises a plurality of VIA headers and the digital signature is generated based on all VIA headers in the SIP headers except a VIA header for the top-listed VIA header.

34. The computer readable medium of claim 32, wherein the plurality of SIP headers comprises a CONTACT header for carrying an address of an endpoint SIP node and a RECORD-ROUTE header for carrying an address of a SIP server, the digital signature being generated based upon at least a portion of the RECORD-ROUTE header.

35. The computer readable medium of claim 34, wherein the digital signature is generated based upon a URI portion of the RECORD-ROUTE header and a URI portion of the CONTACT header.

36. The computer readable medium of claim 32, wherein the digital signature comprises a first signature generated based upon at least a portion of a RECORD-ROUTE header and a second digital signature generated based upon at least a portion of the RECORD-ROUTE header and at least a portion of a CONTACT header of the SIP request.

37. A method of verifying a Session Initiation Protocol (SIP) message, the method comprising:

(a) receiving a SIP response at a SIP node, the SIP response including a message header;

(b) identifying an echoed header in the message header;

(c) extracting a received signature from the echoed header;

(d) generating a verification signature based upon at least a portion of the message header;

(e) comparing the verification signature with the received signature.

38. The method of claim 37, wherein the echoed header is selected from the group consisting of a VIA header, a FROM header, a TO header, a RECORD-ROUTE header, a CALL-ID header, and a CSeq header.

39. The method of claim 38, wherein generating a verification signature includes generating the verification signature based upon at least a portion of at least one of a VIA header, a CONTACT header, a RECORD-ROUTE header, a ROUTE header, a CALL-ID header, and a CSeq header.